

1                    INFORMATION DISTRIBUTION AND PROCESSING

2    FIELD OF THE INVENTION

3    The present invention is directed to a database search  
4    system. More particularly, it is directed to a system for  
5    searching a given database for a given piece of data.

6    BACKGROUND ART

7    In data communication, usually it is necessary to specify  
8    the address of recipients of content. The content cannot be  
9    sent by specifying attributes of the recipients, like "such  
10   and such a person." In multicasting, on the other hand, a  
11   recipient can specify the sender (multicast address) of the  
12   content to receive the content. However, whether a  
13   recipient is allowed to receive the content cannot be  
14   specified by using attributes of the recipient.

15   Today, there are demands for personalized information  
16   (advertisements) and there are many occasions that require  
17   exchange of information adapted to personal attributes.  
18   Therefore, there is need for a content distribution system  
19   in which, rather than directly specifying the addresses of  
20   recipients, a combination of attributes is specified as  
21   criteria so that only those people who meet the criteria can  
22   receive the content. For example, in such a system,  
23   criteria such as {gender = male, age = over 30, occupation =  
24   office worker, hobby = travel} may be described and  
25   recipients, who have registered attributes that meet the

1 criteria can receive the content.

2 On the other hand, privacy protection is important and  
3 personal attributes are the very information that must be  
4 protected.

5 A typical attribute management system for authentication and  
6 personalization is Passport from Microsoft Corporation in  
7 the U.S.A., (MS Passport). In this system, a single server  
8 manages personal information, such as account numbers, about  
9 all users. The information is provided to the server,  
10 subject to the approval of the users. The information is  
11 encrypted before it is transmitted.

12 A problem with the prior-art attribute management systems  
13 such as Passport from Microsoft Corporation described above  
14 is that it relies on a server that manages all personal  
15 information, entailing complete reliance of the users on the  
16 server (and its administrator). This means that in the  
17 event that the server attempts to illegally leak personal  
18 information about users, the users cannot prevent the  
19 leakage.

20 Even if the server is properly managed, the personal  
21 information can be leaked by attack from outside the system  
22 because the server provides a single target of attack,  
23 namely a single attack point.

#### 24 SUMMARY OF THE INVENTION

25 Therefore, the present invention provides systems, apparatus  
26 and methods for an information distribution system in which,

1    instead of directly specifying the addresses of recipients,  
2    a combination of attributes is specified as criteria to  
3    allow only those who meet the criteria to receive the  
4    content while preventing leakage of personal attribute  
5    information to third parties, including the sender,  
6    throughout the process involved in the submission of the  
7    content.

8    The present invention achieving the object is implemented as  
9    an information distribution system characterized by the  
10   following configuration. The information distribution  
11   system comprises a (1) key management server for managing  
12   secret keys and public keys corresponding to given attribute  
13   values; (2) a user terminal accessing a key management  
14   server to obtain attribute secret keys generated based on  
15   secret keys, attribute secret keys corresponding to  
16   attributes of its own; (3) and a provider terminal for  
17   generating an encrypted content that can be decrypted by a  
18   user terminal having a attribute secret keys corresponding  
19   to given attributes by means of a public keys; wherein a  
20   provider terminal distributes a encrypted content and a user  
21   terminal decrypts a encrypted content decryptable by means  
22   of the attribute secret keys of its own.

23   Furthermore, the present invention maybe implemented as a  
24   specific information distribution system comprising: a  
25   service provider for managing secret keys and public keys  
26   for given attribute values; and a plurality of user  
27   terminals for accessing the service provider to obtain  
28   attribute secret keys corresponding to attributes of their  
29   own, the attribute secret keys being generated based on the  
30   secret keys; wherein, a given one of the user terminals  
31   generates an encrypted content and sends the encrypted

1 content to one or more of the other user terminals, the  
2 encrypted content being decryptable by the one or more of  
3 the other user terminals having the attribute secret keys  
4 corresponding to given attributes by means of the public  
5 keys; and the one or more of the other user terminals  
6 decrypt the encrypted content decryptable by means of the  
7 attribute secret keys of their own.

8 BRIEF DESCRIPTION OF THE DRAWINGS

9 These and other aspects, objects, features, and advantages  
10 of the present invention will become apparent upon further  
11 consideration of the following detailed description of the  
12 invention when read in conjunction with the drawing figures,  
13 in which:

14 Fig. 1 is a diagram showing a general configuration of an  
15 information distribution system according to the present  
16 invention;

17 Fig. 2 shows an example of a configuration of an attribute  
18 key management server, a provider terminal, and a user  
19 terminal according to an embodiment;

20 Fig. 3 is a diagram showing a protocol for distributing an  
21 attribute secret key by using k-out-of-n-OT according to the  
22 embodiment;

23 Fig. 4 is a diagram showing a criteria key generation  
24 protocol according to the embodiment;

1 Fig. 5 shows distribution of a content according to the  
2 embodiment;

3 Fig. 6 shows a schematic diagram of an exemplary hardware  
4 configuration of a computer suitable for implementing the  
5 attribute key management server, provider terminal, and user  
6 terminal according to the embodiment;

7 Fig. 7 shows a configuration of a personalized-electronic-  
8 mail distribution service system to which the information  
9 distribution system of the embodiment is applied;

10 Fig. 8 shows a configuration of a distributed matching  
11 service system to which the information distribution system  
12 of the embodiment is applied;

13 Fig. 9 shows an arrangement of distributed search to which  
14 the information distribution system of the embodiment is  
15 applied; and

16 Fig. 10 shows an overview of an arrangement of a community  
17 key generation method using the information distribution  
18 system according to the embodiment.

19 DESCRIPTION OF SYMBOLS

20           10 ... Attribute key management server  
21           11 ... Attribute key generator  
22           12 ... Attribute key storage  
23           20 ... Provider terminal  
24           21 ... Encrypted content generator  
25           22 ... Criteria key generator

1           30 ... User terminal  
2           31 ... Attribute secret key storage  
3           32 ... Decryptor

4       DESCRIPTION OF THE INVENTION

5       The present invention provides systems, apparatus and  
6       methods for an information distribution system in which,  
7       instead of directly specifying the addresses of recipients,  
8       a combination of attributes is specified as criteria to  
9       allow only those who meet the criteria to receive the  
10       content while preventing leakage of personal attribute  
11       information to third parties, including the sender,  
12       throughout the process involved in the submission of the  
13       content.

14       In an example embodiment, the present invention is  
15       implemented as an information distribution system  
16       characterized by the following configuration. The  
17       information distribution system comprises a (1) key  
18       management server for managing secret keys and public keys  
19       corresponding to given attribute values; (2) a user terminal  
20       accessing a key management server to obtain attribute secret  
21       keys generated based on secret keys, attribute secret keys  
22       corresponding to attributes of its own; and (3) a provider  
23       terminal for generating an encrypted content that can be  
24       decrypted by a user terminal having a attribute secret keys  
25       corresponding to given attributes by means of a public keys,  
26       wherein a provider terminal distributes a encrypted content  
27       and a user terminal decrypts a encrypted content decryptable  
28       by means of the attribute secret keys of its own.

1 In the example embodiment, the key management server  
2 comprises a key storage for storing secret keys and public  
3 keys corresponding to predetermined attribute values; an  
4 attribute secret key generator for obtaining a set of given  
5 attribute values and generating attribute secret keys  
6 corresponding to the set of attribute values based on secret  
7 keys corresponding to the attribute values among secret keys  
8 stored in a key storage; and a sending/receiving unit for  
9 receiving the set of attribute values from a given user  
10 terminal and sending the attribute secret keys generated by  
11 the attribute secret key generator to the user terminal.

12 The provider terminal comprises a criteria key generator for  
13 obtaining public keys corresponding to attribute values  
14 indicating attributes of a recipient to which a content is  
15 to be sent and using the public keys to generate criteria  
16 keys that can be decrypted by secret keys corresponding to  
17 the public keys; an encrypted content generator for  
18 encrypting the content based on the criteria keys; and a  
19 sending unit for sending the encrypted content without  
20 specifying any recipient of the content.

21 The criteria key generator combines based on predetermined  
22 rules criteria keys corresponding to the individual  
23 attribute values encrypted by using public keys  
24 corresponding to the individual attribute values to generate  
25 a criteria key for restricting recipients of the content.

26 The user terminal comprises a sending/receiving unit for  
27 accessing a key management server managing secret keys and  
28 public keys corresponding to given attribute values to  
29 receive attribute secret keys corresponding to attributes  
30 established for the information processing apparatus, the

1 attribute secret keys being generated based on the secret  
2 keys; and a decryptor for obtaining an encrypted content and  
3 decrypting the content based on the attribute secret keys.

4 The sending/receiving unit sends a set of attribute values  
5 indicating attributes established for the information  
6 processing apparatus to the key management server and  
7 receives the attribute secret keys generated based on the  
8 set of attribute values from the key management server.

9 The present invention can be implemented as a program for  
10 controlling a computer to function as the key management  
11 server, provider terminal, and user terminal described  
12 above. The program can be stored on a magnetic disc,  
13 optical disc, semiconductor memory, or other storage medium  
14 and distributed, or can be distributed over a network to  
15 provided. Furthermore, the present invention may be  
16 implemented as a specific information distribution system as  
17 described below.

18 An information distribution system comprises a service  
19 provider for managing secret keys and public keys for given  
20 attribute values; and a plurality of user terminals for  
21 accessing the service provider to obtain attribute secret  
22 keys corresponding to attributes of their own, the attribute  
23 secret keys being generated based on the secret keys;  
24 wherein, a given one of the user terminals generates an  
25 encrypted content and sends the encrypted content to one or  
26 more of the other user terminals, the encrypted content  
27 being decryptable by the one or more of the other user  
28 terminals having the attribute secret keys corresponding to  
29 given attributes by means of the public keys; and the one or  
30 more of the other user terminals decrypt the encrypted

1 content decryptable by means of the attribute secret keys of  
2 their own.

3 An alternate information distribution system according to  
4 the present invention, comprises a key management server for  
5 managing secret keys and public keys for given attribute  
6 values; and a plurality of user terminals for accessing the  
7 key management server to obtain attribute secret keys  
8 corresponding to attributes of their own, the attribute  
9 secret keys being generated based on the secret keys;  
10 wherein a given one of the user terminals generates a group  
11 key and sends the group key to ones of the other user  
12 terminals and provides a content, the group key being  
13 decryptable by the ones of the other user terminals having  
14 the attribute secret keys corresponding to given attributes  
15 by means of the public keys, the content being only  
16 accessible by using the group key.

17 Figure 1 illustrates a general configuration of an  
18 information distribution system according to an example  
19 embodiment. Referring to Figure 1, the information  
20 distribution system of the present embodiment comprises an  
21 attribute key management server 10 that manages attribute  
22 keys used for specifying attributes, a provider terminal 20,  
23 which is the sender of contents (information), and user  
24 terminal 30, which are recipients of the contents.

25 The attribute key management server 10, provider terminal  
26 20, and user terminals 30 are implemented by workstations or  
27 personal computers, or other computers having network  
28 capabilities. The user terminals 30 may be information  
29 terminals such as PDAs (personal digital assistants) and  
30 cellular phones that have network capabilities. These

1 devices exchange data over a network, which is not shown.  
2 The communication links of the network may be wired or  
3 wireless.

4 Figure 6 schematically shows a hardware configuration of a  
5 computer suitable for implementing the attribute key  
6 management server 10, provider terminal 20, and user  
7 terminals 30 according to the present embodiment. The  
8 computer shown in Figure 6 comprises a CPU (Central  
9 Processing Unit) 101, which is an arithmetic/logic unit, a  
10 main memory 103 connected to the CPU 101 through an M/B  
11 (mother board) chip set 102 and a CPU bus, a video card 104  
12 also connected to the CPU 101 through the M/B chip set 102  
13 and an AGP (Accelerated Graphics Port), a hard disc 105  
14 connected to the M/B chip set 102 through a PCI (Peripheral  
15 Component Interconnect) bus, and a floppy disc drive 109 and  
16 keyboard/mouse 110 which are connected with the M/B chip set  
17 102 through the PCI bus, a bridge circuit 108 and a  
18 low-speed bus such as an ISA (Industry Standard  
19 Architecture) bus.

20 The hardware configuration of the computer for implementing  
21 the present embodiment shown in Figure 1 is merely  
22 illustrative. Various other configurations to which the  
23 present embodiment can be applied may be used. For example,  
24 a discrete video memory may be provided instead of the video  
25 card 104 and the CPU 101 may process image data.  
26 Furthermore, a CD-ROM (Compact Disc Read Only Memory) and  
27 DVD-ROM (Digital Versatile Disc Read Only Memory) drives may  
28 be attached through an interface such as an ATA (AT  
29 Attachment).

30 The provider terminal 20 in Figure 1, specifies attributes

1 for identifying the recipients of a content and sends the  
2 content to their user terminals 30. Attribute keys provided  
3 by the attribute key management server 10 are used for  
4 specifying the attributes. Attribute keys are keys (secret  
5 key and public key) established for attributes that can be  
6 specified in communication from the provider terminal 20 to  
7 the user terminals 30. The user terminals 30 may obtain any  
8 number of attribute keys for their attributes from the  
9 attribute key management server 10. Thus, the provider  
10 terminal 20 multicasts a content to the user terminals 30.

11 The assumption in this embodiment is that attributes and  
12 possible values of the attributes (attribute values) are  
13 predetermined. The term attribute as used herein refers to  
14 information representing the individuality of the user of a  
15 user terminal 30 or the user terminal itself. Various types  
16 of information can be set as the attributes according to the  
17 form and operation of the system used with the present  
18 embodiment. Let a set (size =  $n_i$ ) of values that a given  
19 attribute  $A_i$  can take be  $V_i = \{v_{i,1}, v_{i,2}, \dots, v_{i,n}\}$ . Because  
20 some attributes can take on a plurality of values, the  
21 generalization is made that the number of values that an  
22 attribute can take is  $k_i (\leq n_i)$ . These are specific to each  
23 attribute. For example, if attribute  $A_1$  is gender, the set  
24 of values it can take is  $V_1 = \{\text{male}, \text{female}\}$  and therefore  
25  $n_1 = 2$  and  $k_1 = 1$ .

26 Attribute criteria are described as follows. That the value  
27 of a given attribute  $A_i$  is  $v_i$  is written  $A_i (v_i)$ .  
28 Furthermore, AND and OR operators, &, |, and parentheses ()  
29 are used. For example, attributes {gender = male, age =  
30 30's, occupation = office worker, hobby = travel or PC  
31 operation} are written as follows:

1           gender (male) & age (30's) & occupation (office worker)  
2           & (hobby (travel) | hobby (PC operation)).

3       Furthermore, in the following description,  $p$  is a large  
4       prime,  $q$  is a prime that can divide  $p-1$ , and  $g$  is an element  
5       of the order  $q$  in a finite field  $Z_p$ . All the arithmetic  
6       operations are performed in  $Z_p$  unless otherwise stated.

7       Figure 2 shows a configuration of the attribute key  
8       management server 10, the provider terminal 20, and a user  
9       terminal 30 according to the present embodiment. Referring  
10      to Figure 2, the attribute key management server 10  
11      comprises an attribute key generator 11 for generating  
12      attribute keys and an attribute key storage 12 for storing  
13      the generated attribute keys. The attribute key generator  
14      11 generates a secret key and a public key for each of  
15      attribute predetermined as attribute keys and generates  
16      secret keys (attribute secret keys) corresponding to  
17      individual attributes of individual user terminals 30 by  
18      communicating with them. The generated attribute secret  
19      keys unique to the user terminals 30 are sent to those user  
20      terminals 30.

21      The attribute key generator 11 is a virtual software block  
22      implemented by the CPU 101 under the control of a program in  
23      the computer constituting the attribute key management  
24      server 10. The attribute key storage 12 is implemented by a  
25      storage device (magnetic disc device, optical disc device,  
26      semiconductor memory, or the like) of the computer  
27      constituting the attribute key management server 10. The  
28      attribute key management server 10 also includes a  
29      sending/receiving unit, which is not shown, implemented by

1 the program-controlled CPU 101 and network a network  
2 interface 106.

3 The provider terminal 20 comprises an encrypted content  
4 generator 21 for encrypting contents to be distributed and a  
5 criteria key generator 22 for generating criteria keys used  
6 for decrypting encrypted contents. The encrypted content  
7 generator 21 encrypts a content itself with a common key  
8 known as a session key. The criteria key generator 22  
9 generates a key including information for encrypting and  
10 decrypting a session key as the criteria key, rather than  
11 generating a key for directly decrypting the content.

12 The encrypted content generator 21 and the criteria key  
13 generator 22 are virtual software blocks implemented by a  
14 program-controlled CPU 101 in the computer constituting the  
15 provider terminal 20. The provider terminal 20 includes a  
16 sending/receiving unit implemented by the program-controlled  
17 CPU 101 and a network interface 106.

18 The user terminal 30 comprises an attribute secret key  
19 storage 31 for holding an attribute secret key unique to the  
20 user terminal 30 that is obtained from the attribute key  
21 management server 10 and a decryptor 32 for decrypting  
22 encrypted contents distributed from the provider terminal 20  
23 with the attribute secret key stored in the attribute secret  
24 key storage 31.

25 The attribute secret key storage 31 is implemented by a  
26 storage device (magnetic disc device, optical disc device,  
27 semiconductor memory or the like) of the computer or  
28 information terminal constituting the user terminal 30. The  
29 decryptor 32 is a virtual software block implemented by a

1 program-controlled CPU 101. The user terminal 30 includes a  
 2 sending/receiving unit, which is not shown, implemented by  
 3 the program-controlled CPU 101 and a network interface 106.  
 4 An example of a protocol used for implementing the  
 5 information distribution system according to the  
 6 embodiment includes the following three phases:  
 7       1. Generation and distribution of attribute keys as  
 8       preprocessing,  
 9       2. Generation of criteria keys by the provider  
 10       terminal 20, and  
 11       3. Distribution of contents through multicasting.  
 12       Each of these phases will be described in detail below.

13 1. Generation and distribution of attribute keys

14 The attribute key generator 11 of the attribute key  
 15 management server 10 selects an attribute secret key  $s_{i,j}$  at  
 16 random for each value in a set of attribute values  $\{v_{i,1},$   
 17  $v_{i,2}, \dots, v_{i,n}\}$  for registered attributes  $A_i$  and publishes an  
 18 attribute public key

19  $y_{i,j} = g^{s_{i,j}} \pmod{p}$  [Equation 1].

20 The user terminal 30 communicate with the attribute key  
 21 management server 10 and performs Oblivious Transfer (herein  
 22 after abbreviated to OT) to secretly obtain attribute secret  
 23 keys for attribute values of itself without being known to  
 24 the attribute key management server 10. OT is a protocol  
 25 between two parties, an information provider and an  
 26 information selector, in which the selector selects and  
 27 obtains some pieces of information held by the provider.  
 28 Here, the following two conditions must be met:  
 29       (1) Privacy of the selector: the provider is not

1       allowed to know which information is selected by the  
2       selector, and

3       (2) Privacy of the provider: the selector is not  
4       allowed to know other information than the selector  
5       selected.

6       OT is disclosed in the following literature:

7       M. Bellare and S. Micali, Non-interactive oblivious  
8       transfer and applications, Advances in Cryptology ---  
9       Crypto '89, pp. 547-557, 1990.

10      One basic OT is 1-out-of-2-OT. In this OT, a provider has  
11      two pieces of information and a selector selects one of  
12      them. A typical protocol to achieve this is one that uses  
13      ElGamal encryption. This protocol will be described below.  
14      Here, let the pieces of information held by the provider be  
15       $I_0, I_1$  and the value selected by the selector be  $b \in \{0,1\}$ ,  $\sim b$   
16      = NOT  $b$ .

17           (1) The information provider generates a random number  
18            $r$  and sends it to the selector,  
19           (2) The selector uses the random number  $r$  it received  
20           to generate  $K_b = g^x$ ,  $K_{\sim b} = r/K_b$  and sends it to the  
21           information provider,  
22           (3) The information provider checks to see if  $K_0 * K_1 = r$   
23           (4) The information provider generates an encrypted  
24           content  $\{E_{I1}, E_{I2}\}$  and sends it to the selector, where  
25            $E_{I1} = (g^h, I_0 * K_0^h)$  and  $E_{I2} = (g^h, I_1 * K_1^h)$ , and  
26           (5) The selector decrypts the content  $I_b$ .

27      1-out-of-2-OT protocol has been described above in which one  
28      of two pieces of information is selected. In the present  
29      embodiment, this protocol is expanded to  $k$ -out-of- $n$ -OT, in



1 keys  $S_{ij}$ , each of which is encrypted by  $Y(j)$  as an ElGamal  
2 encryption public key, to the user terminal 30 (there is no  
3 need to use a secret communication link).

4 For verification that the  $n$  points are on the  $k$ -order  
5 polynomial  $K$  points are randomly selected from a set of  $n$   
6 points  $\{Y(1), \dots, Y(n)\}$  to form  $F(x)$ : a polynomial of order  $k$ ,  
7 then check that  $F(o)=Qo$ .

8 (4) The user terminal 30 can decrypt only the  $k$  points  
9 specified by  $h(j)$  ( $1 \leq j \leq k$ ) from (out of)  $n$  ElGamal-encrypted  
10 points, by using the attribute secret key  $s_{ij}$  received from  
11 the attribute key management server 10. Thus, it can obtain  
12  $k$  attribute secret keys.

13 Beside  $k$ -out-of- $n$ -OT described above, attribute secret keys  
14 for numerical attributes are generated by using the  
15 following representation:

16 (1) Let the binary expression of an  $n$ -bit positive integer  $x$   
17 be  $(x_{n-1}, \dots, x_0)$ .

18 (2) The attribute key generator 11 of the attribute key  
19 management server 10 generates  $2n$  pairs of a secret key and  
20 a public key  $\{(pk_j^{(0)}, sk_j^{(0)}), (pk_j^{(1)}, sk_j^{(1)}) \mid j = 0, \dots, n-1\}$   
21 and assigns the two types of secret keys to each bit. That  
22 is, it assigns  $sk_j^{(0)}$  and  $sk_j^{(1)}$  to  $j$ -th bit. It publishes  
23 public keys  $pk_j(0)$  and  $pk_j(1)$  corresponding to them.

24 (3) A user terminal 30 that selects the value  $X = (x_{n-1}, \dots,$   
25  $x_0)$  through the attribute key distribution using  $n$  times  
26 1-out-of-2 OT, which is described earlier, obtains  $(sk_j^{(x_{n-1})},$   
27  $\dots, sk_j^{(x_0)})$ .

1 As described above,  $k$ -out-of- $n$ -OT and, 1-out-of-2 OT for  
2 numerical attributes, are used to distribute attribute  
3 secret keys, which allow the user terminal 30 to obtain  
4 attribute secret keys corresponding to attributes of itself  
5 without allowing even the attribute key management server 10  
6 to know them, that is, without leaking its personal  
7 information.

## 8 2. Criteria key generation

9 The criteria key generator 22 of the provider terminal 20  
10 combines attribute public keys published by the attribute  
11 key management server 10 as below to generate a criteria  
12 key.  $E(PK, K)$  represents that session key  $K$  is encrypted  
13 with public key  $PK$ .  $E_k(M)$  represents that message  $M$  is  
14 encrypted with symmetric key  $K$ .

15 (1) Construction of AND key: Attribute public keys  $y_{ij}$  and  
16  $y_{k1}$  correspond to attribute criteria  $A_i(v_{ij})$  &  $A_k(v_{k1})$ ,  
17 respectively. Two session keys  $K_{ij}$  and  $K_{k1}$  are selected at  
18 random and encrypted with a public key, resulting in a  
19 criteria key  $\{E(y_{ij}, K_{ij}), E(y_{k1}, K_{k1})\}$  and its corresponding  
20 session key  $K = K_{ij} + K_{k1}$ . In addition,  $E(y_{ij}, E(y_{k1}, K))$  is  
21 an encryption constituting AND.

22 (2) Construction of OR key: Attribute public keys  $y_{ij}$  and  $y_{k1}$   
23 correspond to attribute criteria  $A_i(v_{ij}) \mid A_k(v_{k1})$ ,  
24 respectively. One of the session keys  $K$  is selected at  
25 random and encrypted with the two public keys. The  
26 resulting criteria key is  $\{E(y_{ij}, K), E(y_{k1}, K)\}$ .

27 (3) Construction of NOT key: Attribute public keys  $y_{ik}$ ,  $k=1$ ,

1 ...,  $j-1$ ,  $j+1$ , ...,  $n_i$  correspond to attribute criteria  $A_i(v_{ij})$ .  
 2 One session key  $K$  is selected at random and encrypted with  
 3  $n_i-1$  keys. The resulting criteria key is  $E(y_{i1}, K) || \dots || E$   
 4  $(y_{ij-1}, K) || E(y_{ij+1}, K) || \dots || E(y_{ini}, K)$ .

5 (4) Combined AND/OR criteria: Criteria keys and session keys  
 6 for any combinations of AND and OR can be generated by  
 7 repeating the process described above, starting from the  
 8 lowest-level operator, to concatenate criteria keys and  
 9 calculating session keys.

10 Furthermore, consider a case where the provider terminal 20  
 11 wants to allow a content to be decrypted if  $X \geq Y$  holds for a  
 12 given  $n$ -bit positive integer  $Y = (y_{n-1}, \dots, y_0)$ . The criteria  
 13 key generator 22 of the provider terminal 20 calculates  $C =$   
 14  $(c_{n-1}, \dots, c_0)$  as follows. Here,  $k_{n-1}, \dots, k_0$  are random number  
 15 and  $k_0 = K$  is a session key for numerical attribute criteria  
 16  $(X \geq Y)$ .  $c_{n-1}, \dots, c_0$  are determined as follows:

17  $c_j = E(sk^{(1)}_j, k_j)$  if  $y_j = 1$   
 18  $c_j = E(sk^{(0)}_j, K) || E(sk^{(1)}_j, k_j)$  if  $y_j = 0$ .

19 The provider terminal 20 sends a criteria key  $(c_{n-1},$   
 20  $E_{k_{n-1}}(c_{n-2}), \dots, E_{k_1}(c_0))$  to the user terminal 30. The user  
 21 terminal 30 can determine  $k$  if  $X \geq Y$ . Likewise, criteria keys  
 22 for  $X > Y$ ,  $X \leq Y$ , and  $X < Y$  can be generated. Numerical attribute  
 23 criteria generated using this method can be combined to  
 24 generate a criteria key such that  $Y \leq X \leq Y'$ . Figure 4 shows a  
 25 diagram for illustrating the protocol described above.

### 26 3. Distribution through multicasting

27 The provider terminal 20 adds a criteria key generated by  
 28 using the criteria key generation protocol described above

1 to the header of a content, encrypts the body of the content  
2 with a session key generated by using the criteria key  
3 generation protocol, and multicasts the encrypted contents  
4 with the content header. Figure 5 shows a diagram for  
5 explaining the multicasting. Only user terminal 30 having  
6 an attribute secret key that meets the conditions of the  
7 criteria key can decrypt the multicasted content.

8 The information distribution system according to the present  
9 embodiment arranged as described above has the following  
10 main characteristics.

11 (1) Efficiency and off-line characteristics of key  
12 acquisition

13 The user terminal 30 can receive attribute secret keys from  
14 the attribute key management server 10 with the one-round  
15 protocol. Furthermore, once the user terminal 30 obtains  
16 the keys, it can use the keys in any number of subsequent  
17 multicasts.

18 (2) Provider terminal registration not required

19 The provider terminal 20 can use attribute public keys of  
20 the attribute key management server 10 without having to  
21 interacting with the attribute key management server 10.  
22 The attribute public keys can be reused.

23 (3) Off-line nature of attribute key management server 10

24 The attribute key management server 10 involves only in key  
25 acquisition by the user terminal 30. It was not involved in  
26 actual communication. Therefore, any protocols for a  
27 standard multicast such as IP multicast or broad cast can be  
28 used in the actual communication.

1 (4) Openness of recipient group

2 The provider terminal 20 can send a content through a  
3 multicast without knowing the entire recipient group or a  
4 whole set that can receive the content. Conversely, the  
5 user terminal 30 can join the recipient group by receiving  
6 attribute secret keys from the attribute key management  
7 server 10 at any time.

8 A specific example of the information distribution system to  
9 which the present embodiment can be applied will be  
10 described below.

#### 11 1. Personalized electronic mail distribution service

12 There are systems distributing electronic mail to a  
13 plurality of or unspecified users through a service  
14 provider. In such a system, the service provider 700 can  
15 operate an attribute key management server 10 and an  
16 electronic mail sender 710 can act as a provider terminal 20  
17 to distribute electronic mail messages encrypted based on a  
18 criteria key corresponding to given attributes. Figure 7  
19 shows a general configuration of this system.

20 According to the present embodiment, the sender of  
21 electronic mail specifies attributes of recipients of the  
22 mail but cannot know who has the specified attribute.  
23 Therefore, the privacy concerning attributes of the users  
24 can be fully protected. Thus, the users can obtain secret  
25 keys for attributes of themselves and receive personalized  
26 information. Unlike models in conventional database  
27 marketing used by a sender to select recipients by  
28 inference, this system allows the recipients to actively  
29 obtain information that they want, therefore distribution

1 with a higher hit rate can be expected.

## 2 2. Distributed matching service system

3 There are services for a plurality of or unspecified users  
4 to exchange queries and information with each other. One  
5 example is matching service on a network. In matching  
6 service, members, or users, exchange conditions and  
7 information about their profile to find a marriage partner  
8 based on the information. A service provider 800 manages an  
9 attribute key management server 10 and each user terminal  
10 810 acts as a provider terminal 20 as well as a user  
11 terminal 30. A user specifies as attributes conditions and  
12 items of profile information to exchange and exchanges  
13 messages encrypted based on a criteria key corresponding to  
14 the attributes. Therefore, they can exchange the  
15 information with each other with information other than the  
16 exchanged information being completely hidden. Figure 8  
17 shows a general configuration of the system.

## 18 3. Distributed search service system

19 The operator of a search engine site operates an attribute  
20 key management server 10 and registers attributes such as  
21 specialties as keywords. A user terminal 30 obtains its  
22 attribute secret key for its specialty. A questioner 910  
23 equivalent to a provider terminal 20 combines keywords to  
24 construct a question and transmit it over a network. A  
25 given user terminal 30 can decrypt and read the question and  
26 reply to it only if it matches its specialty. Figure 9  
27 shows a general configuration of this system.

## 28 4. Community key generation method

1 Figure 10 shows a general configuration of a community key  
2 generation method using an information distribution system  
3 according to the present embodiment. A network operator  
4 such as an ISP (Internet Service Provider) operates an  
5 attribute key management server 10. It registers attributes  
6 such as topics on a community. The members of the community  
7 use a terminal 1010 acting as a provider terminal 20 as well  
8 as a user terminal 30. They obtain attribute secret keys  
9 for topics of interest to them with a function as the user  
10 terminal 30. A given member combines sets of attribute  
11 criteria at will, hosts a chat room 1020, generates its  
12 group key as a message, encrypts it based on a criteria key  
13 corresponding to the attribute criteria, and distribute it  
14 to the other members. Thus, only the recipients that meet  
15 the attribute criteria can decrypt the group key and join  
16 the chat room 1020. Of course, criteria keys and attribute  
17 secret keys for obtaining various contents on the network  
18 can also be established.

19 Thus, according to the present invention, an information  
20 distribution system is provided in which, instead of  
21 directly specifying the addresses of recipients, a  
22 combination of attributes is specified as criteria to allow  
23 only those who meet the criteria to receive the content  
24 while preventing leakage of personal attribute information  
25 to third parties, including the sender, throughout the  
26 process involved in the submission of the content.

27 Variations described for the present invention can be  
28 realized in any combination desirable for each particular  
29 application. Thus particular limitations, and/or embodiment  
30 enhancements described herein, which may have particular

1 advantages to the particular application need not be used  
2 for all applications. Also, not all limitations need be  
3 implemented in methods, systems and/or apparatus including  
4 one or more concepts of the present invention.

5 The present invention can be realized in hardware, software,  
6 or a combination of hardware and software. A visualization  
7 tool according to the present invention can be realized in a  
8 centralized fashion in one computer system, or in a  
9 distributed fashion where different elements are spread  
10 across several interconnected computer systems. Any kind of  
11 computer system - or other apparatus adapted for carrying  
12 out the methods and/or functions described herein - is  
13 suitable. A typical combination of hardware and software  
14 could be a general purpose computer system with a computer  
15 program that, when being loaded and executed, controls the  
16 computer system such that it carries out the methods  
17 described herein. The present invention can also be  
18 embedded in a computer program product, which comprises all  
19 the features enabling the implementation of the methods  
20 described herein, and which - when loaded in a computer  
21 system - is able to carry out these methods.

22 Computer program means or computer program in the present  
23 context include any expression, in any language, code or  
24 notation, of a set of instructions intended to cause a  
25 system having an information processing capability to  
26 perform a particular function either directly or after  
27 conversion to another language, code or notation, and/or  
28 reproduction in a different material form.

1     Thus the invention includes an article of manufacture which  
2     comprises a computer usable medium having computer readable  
3     program code means embodied therein for causing a function  
4     described above. The computer readable program code means  
5     in the article of manufacture comprises computer readable  
6     program code means for causing a computer to effect the  
7     steps of a method of this invention. Similarly, the present  
8     invention may be implemented as a computer program product  
9     comprising a computer usable medium having computer readable  
10    program code means embodied therein for causing a a function  
11    described above. The computer readable program code means  
12    in the computer program product comprising computer readable  
13    program code means for causing a computer to effect one or  
14    more functions of this invention. Furthermore, the present  
15    invention may be implemented as a program storage device  
16    readable by machine, tangibly embodying a program of  
17    instructions executable by the machine to perform method  
18    steps for causing one or more functions of this invention.

19    It is noted that the foregoing has outlined some of the more  
20    pertinent objects and embodiments of the present invention.  
21    This invention may be used for many applications. Thus,  
22    although the description is made for particular arrangements  
23    and methods, the intent and concept of the invention is  
24    suitable and applicable to other arrangements and  
25    applications. It will be clear to those skilled in the art  
26    that modifications to the disclosed embodiments can be  
27    effected without departing from the spirit and scope of the  
28    invention. The described embodiments ought to be construed

1 to be merely illustrative of some of the more prominent  
2 features and applications of the invention. Other  
3 beneficial results can be realized by applying the disclosed  
4 invention in a different manner or modifying the invention  
5 in ways known to those familiar with the art.